网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

资源代价与安全算力

移动终端高级威胁的新挑战及对抗发现

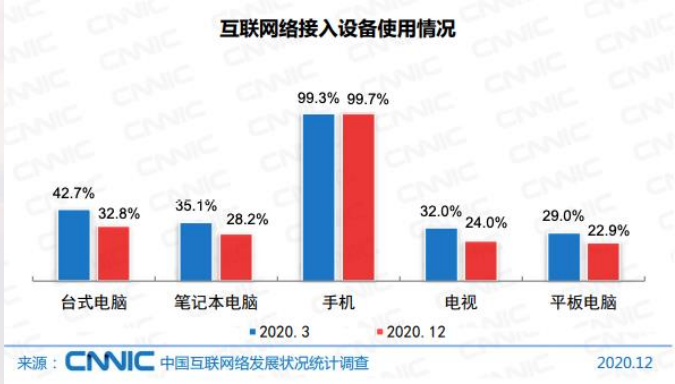
安天 | 移动威胁情报中心

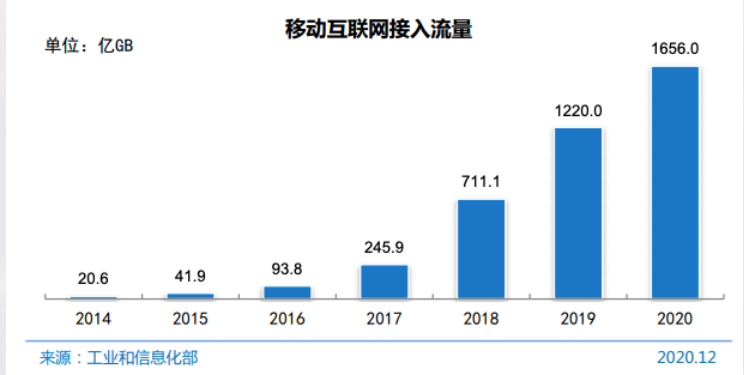
CONTENTS

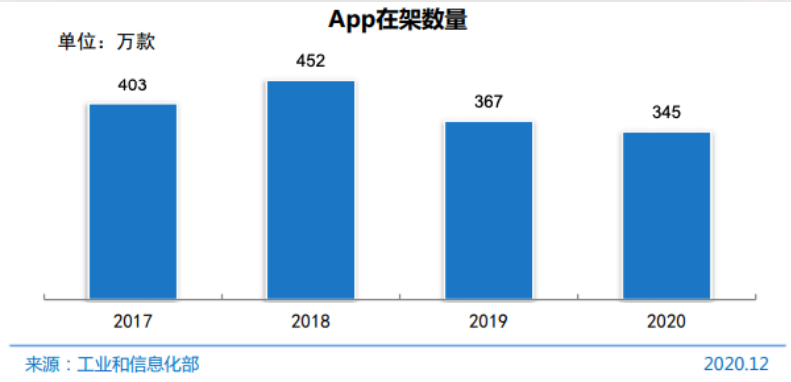
目 录

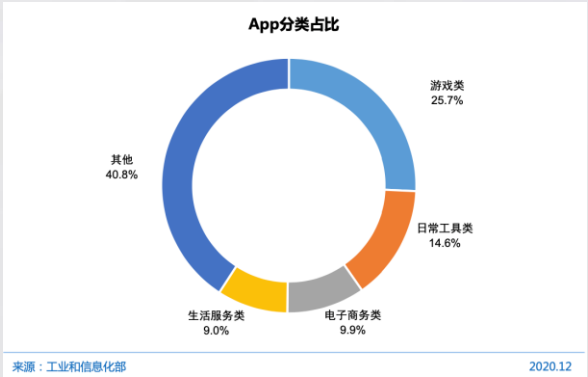
01 移动端威胁的新挑战

移动互联网发展趋势







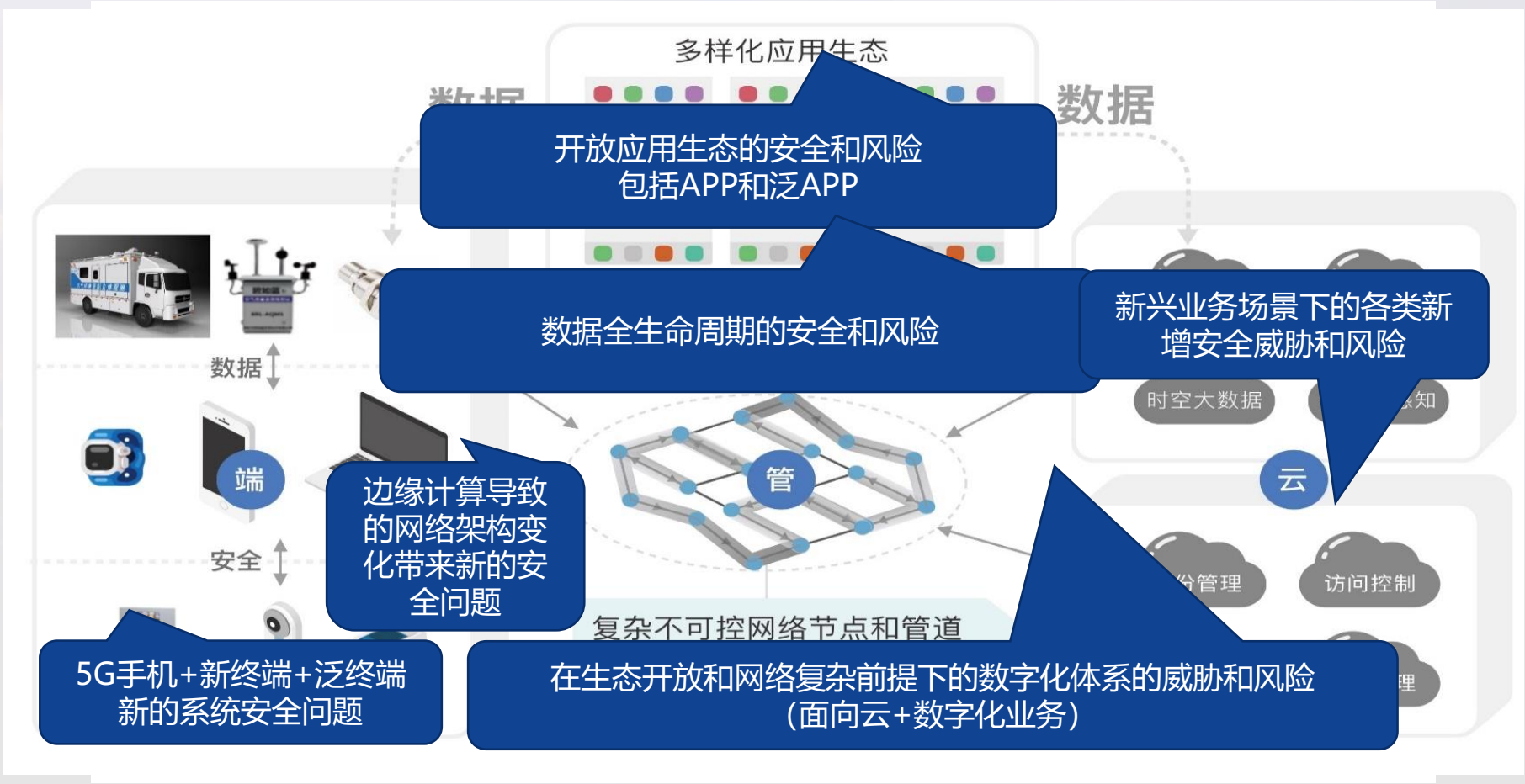


移动办公：

钉钉用户：5亿

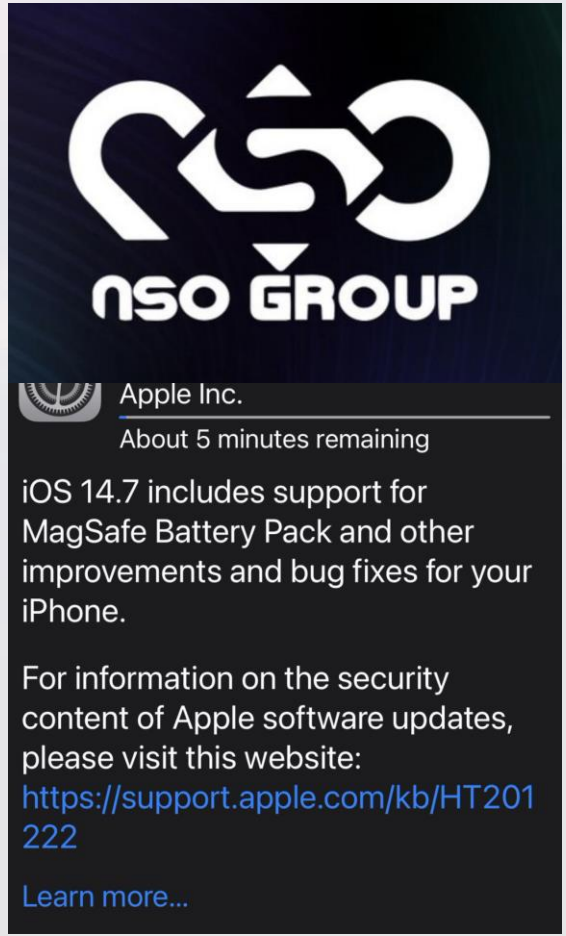
企业微信用户： 1.8亿

生态开放和复杂网络下的数字化体系普遍威胁

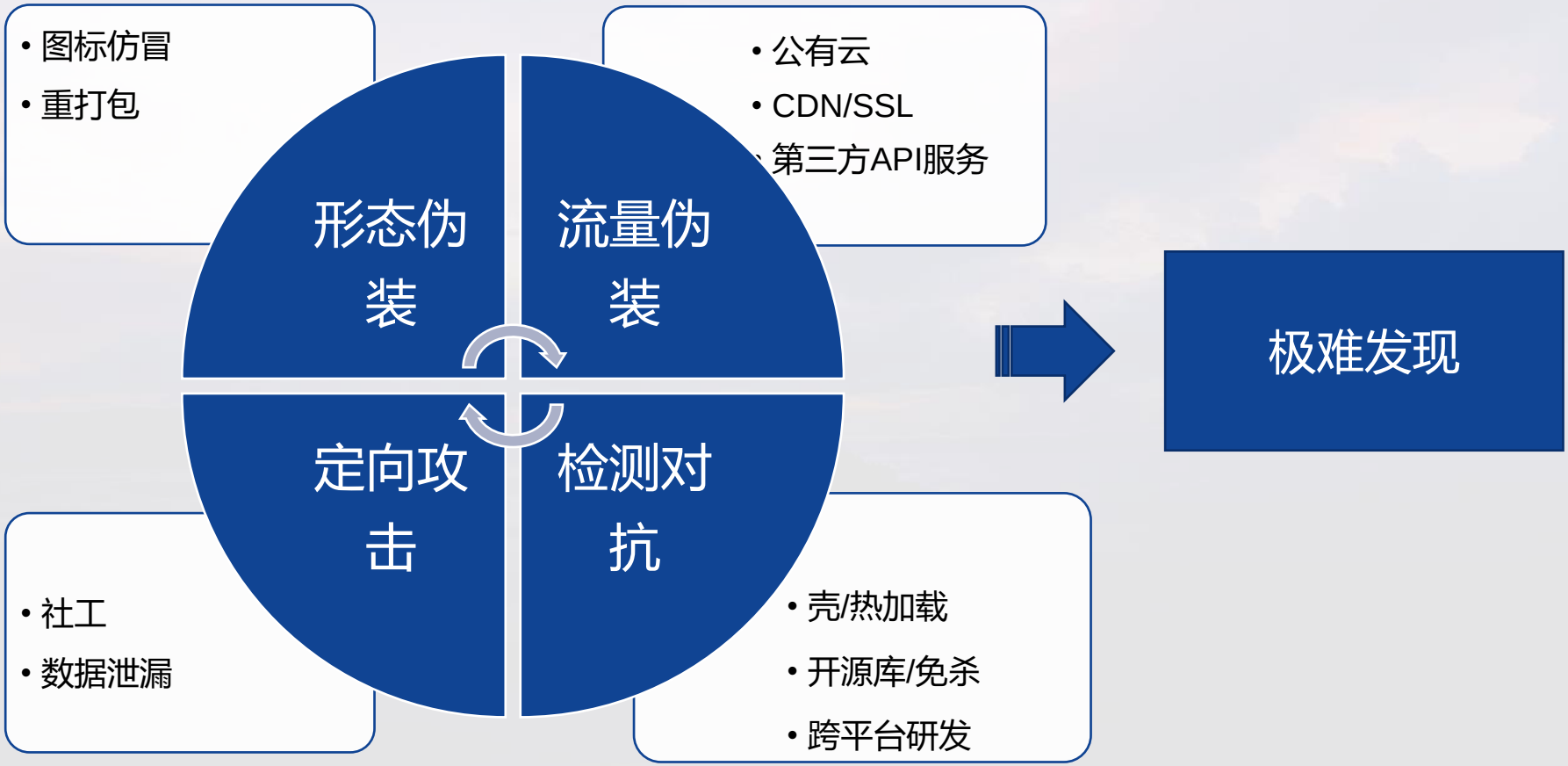


移动攻击能力成为全球apt组织和军火商标配

没有安全的系统：移动端攻击武器具备高强的漏洞使用能力



伪装和隐藏手段层出不穷



恶意载荷制作愈加精美

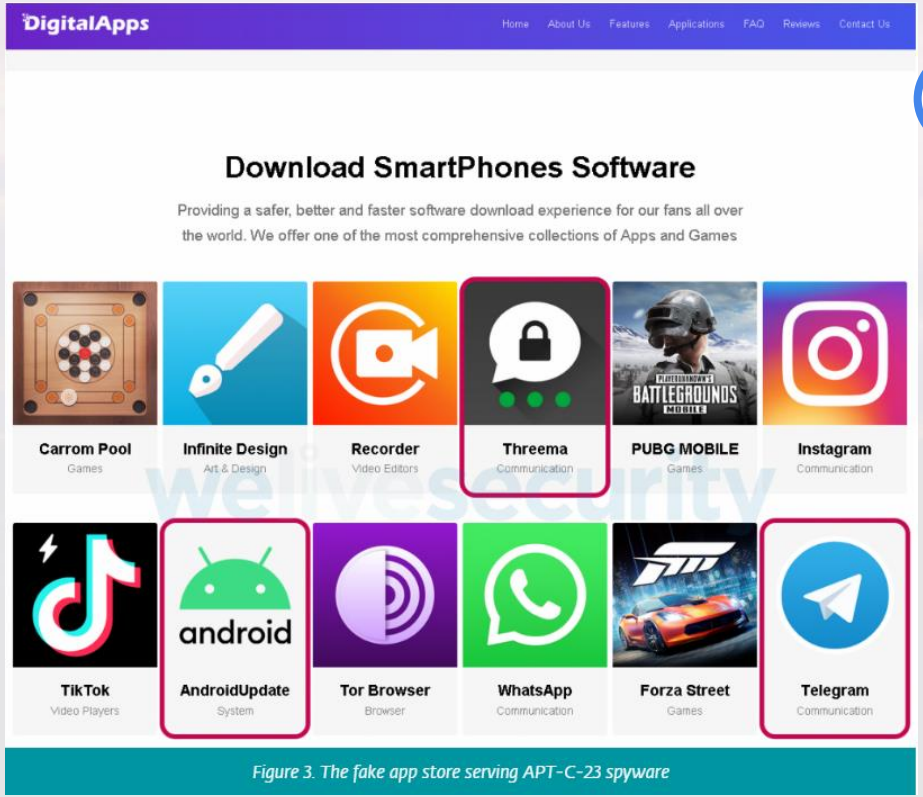
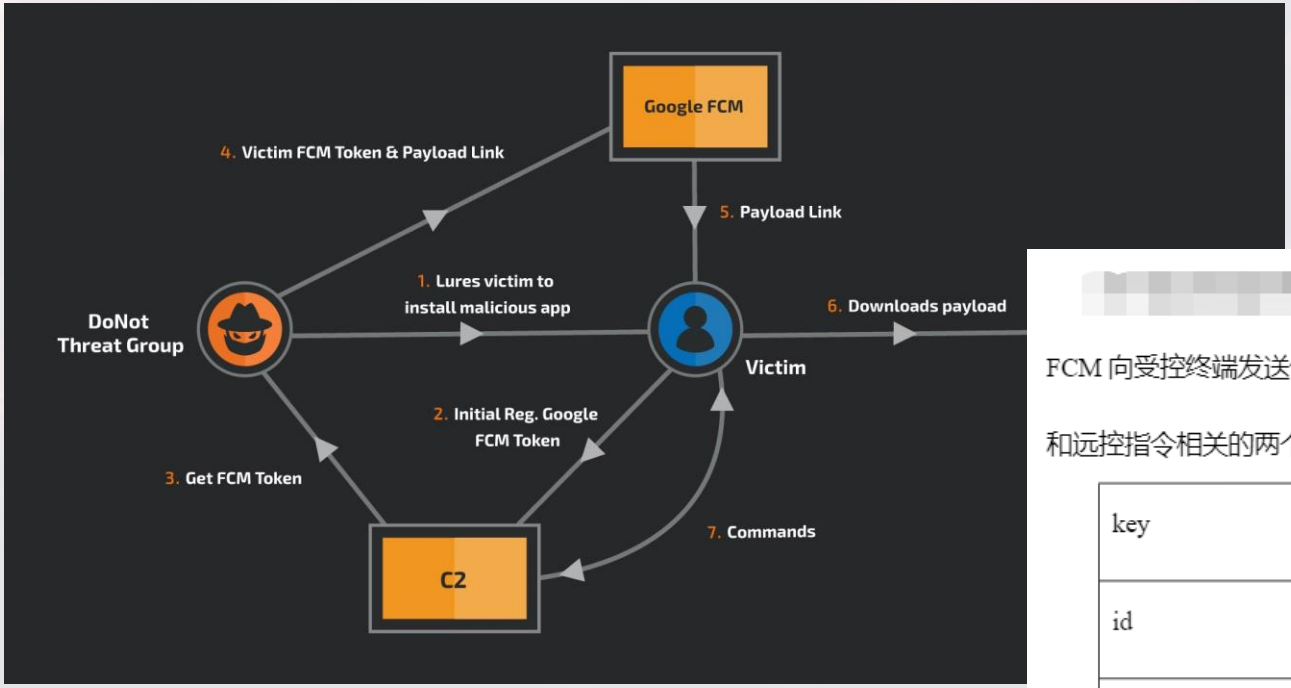


Figure 3. The fake app store serving APT-C-23 spyware

为恶意载荷投放制作“官网”以及放置了大量正版应用的应用商店

云服务成攻击组织首选基础设施



DoNot

双尾蝎

该样本还能通过 FCM 向受控终端发送控制指令。攻击者通过 FCM 向受控终端发送包含控制指令的数据集合，这些数据以 map 集合的形式发送。其中和远控指令相关的两个键值为：

key	value 的含义
id	任务 ID，不同的 ID 用于执行不同的任务
type	远程控制的任务类型

动态更换C2地址

存放各种加密字符串

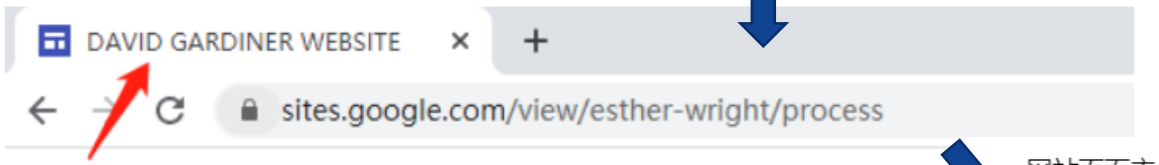
```
&v4,
(int)"3K=H8N=O7S=H8A=N-unjwgXJvxg8rvHlk3bv85GGXmzfCRmbAzGtF2XLtd/0m9pzxv5dYqNSfXFoNYGPdPmvJIQjwiWOYA9LtSyOvMA==");
 = (const char *)sub_8E80(&v4);
v3 = _JNIEnv::NewStringUTF(a1, v1);
```

加密后的sites.google.com/xxxxxxx 字符串

```
try {
    try {
        v4 = c.f.a.a.a("PUNCAPT_DROPTOLL", Appcontroller.l.substring(Appcontroller.l.indexOf("-") + 1)).replaceAll(" ", "t").replaceAll("twitter", "google").replaceAll("8", "s");//返回解密后的url
        goto label_28;
```

解密函数

从so文件中得到的加密字符串



网站页面主体一片空白，真正的 C2 地址隐藏在网站标题中。样本获取网站标题后，

通过一定的算法组合成 C2 地址，组合算法为：

```
v0 = arg8.substring(arg8.indexOf(">") + 1).trim().replaceFirst(v0, "-").replaceFirst(v0, ".").toLowerCase();
```

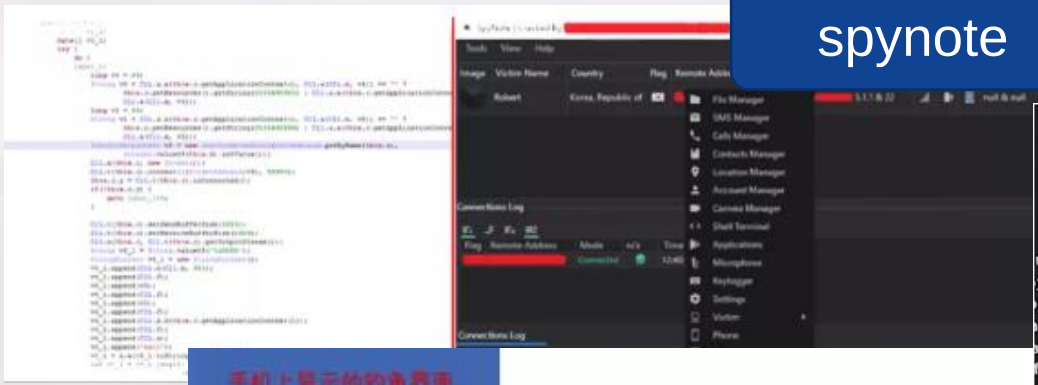
```
url_c2 = title.substring(title.indexOf(">") + 1).trim().replaceFirst(" ", "-").replaceFirst(" ", ".").toLowerCase();
```

组合后得到的 C2 地址为：https://d[redacted]er.wel[redacted]

增加静态分析难度
随时更换C2地址

开源间谍木马框架被广泛利用

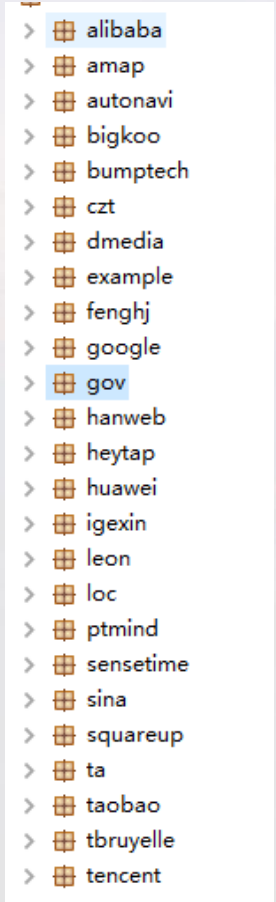
spynote



loadRAT

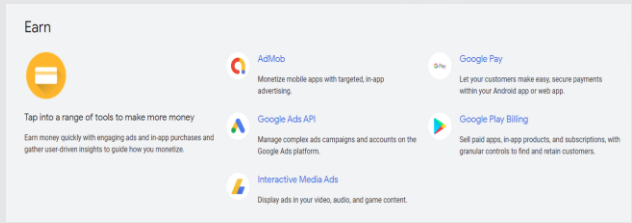
GAZA007

高度依赖SDK移动应用存在严重的供应链攻击隐患



- Visit SDK(Reveal Mobile)分析
- Krux SDK (Audience Studio)分析
- Gimbal SDK分析
- Ninthdecimal SDK分析
- Skyhook SDK分析
- Tamoco SDK分析
- Tutela SDK分析
- Unacast SDK分析
- Cuebig SDK分析
- Near SDK分析
- PlacedFourSquare SDK分析
- Place IQ SDK分析
- Safegraph SDK分析
- Teemo SDK分析

SDK横向穿透突破了监管单位构建的app分类监管的数据锁



01.法规/标准

《常见类型移动互联网应用程序必要个人信息范围规定》《个人信息保护法》收集最小必要原则

02.寄生共享

SDK寄生在APP内部，数据获取权限与APP共享，且具有隐形合法效果

03.突破数据锁

单一SDK嵌入不同类别APP实现多类数据收集和关联，打破监管最小化获取用户数据的保护措施

02 移动供应链的威胁情况分析

基于应用SDK的画像能力是移动APT的新形态

用户规模性 → 细分标签体系 → 整合多家数据 → 形成大数据能力

- 新加坡的移动营销平台 ADTiming，其合作遍布全球 40+ 国家与地区
- 通过人群分组技术细分出 30000+ 个广告标签
- 整合多家广告平台的数据资源
- 打破孤岛效应，对人群画像做到非常细致
- 《纽约时报》报导通过1200万部手机、500亿个**实时位置数据**可以跟踪特朗普一天的行踪
- 美国Anomaly Six声称他们的SDK嵌入全球超过**500款**软件，可以对全球数亿用户的位置信息进行跟踪

境外SDK厂商收集数据赋能情报机构

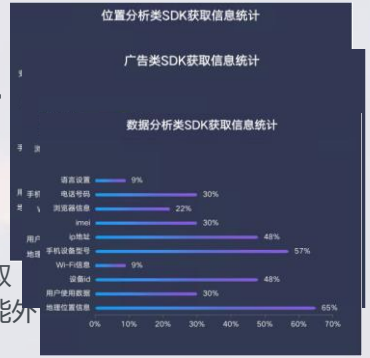
具备获取用户位置境外SDK厂商

境外SDK多具位置收集能力

- 数据收集占比高
- 数据类型多种多样
- 用户覆盖范围广

境外SDK收集数据类型广泛

- 境外位置类SDK获取
- 境外广告类SDK信息获取
- 境外数据分析类SDK信息获取
- 大部分SDK除了满足自身功能外
- 还额外进行其他功能收集



境外SDK收集数据统计


THE WALL STREET JOURNAL.

Apple and Google to Stop X-Mode From Collecting Location Data From Users' Phones

After the data broker came under scrutiny for national-security work, tech giants tell app developers to remove trackers or lose access to their operating systems

MOST POPULAR VIDEOS

多家厂商与美国安全部门合作

与情报组织合作广泛

- 美国特种陆战队购买Babel Street公司的**位置数据**服务
- X-Mode公司的客户包含美国情报部门

具备各类敏感信息收集能力

- 安天对国内百余款APP进行分析统计，发现超过半数的境外SDK获取用户的地理位置
- 有相当多的一部分收集用户的**终端指纹**和**行为数据**

SDK 名称	所属公司功能业务	公司所在地
Google tag manager	统一的广告和分析平台，用于更智能的营销和更好的结果	美国
Facebook share	人工智能、虚拟现实、机器学习、社交媒体、增强现实、营销科学、移动连通性和开放计算	美国
Facebook analytics	人工智能、虚拟现实、机器学习、社交媒体、增强现实、营销科学、移动连通性和开放计算	美国
FacebookAds	人工智能、虚拟现实、机器学习、社交媒体、增强现实、营销科学、移动连通性和开放计算	美国

境外SDK收集境内设备信息

境外情报组织通过大数据画像，可实现对境内目标进行差别攻击

境内3.8亿部手机安装了使用境外sdk的应用程序

各类应用都有使用境外sdk

谷歌等大厂sdk使用广泛

美国SDK服务商占据主导地位

渗透能力

- 全球SDK市场，美国占据领先地位（用户群体上）
- 美国互联网巨头服务商，除了**自身产品**外还有**自研SDK**嵌入其他APP；
- 美国几乎通过自己国家的SDK服务商从而**掌握全球移动用户的数据**

威胁能力

- 细分领域使用境外SDK，具有**未知风险**?
- 境外的数据收集真的**单纯用在具体业务**上?

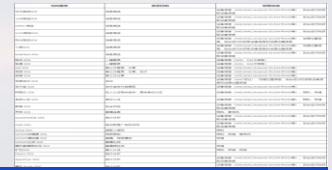
合法外衣下的境外SDK数据风险案例

合法收集

国内合法主体公司经营

- 分析师发现小红书使用Amazon**境内的服务**节点作为用户笔记数据的处理和存放供应商
- 网易邮箱集成了境外SDK InMobi，其在国内的运营主体名叫邑盟信息技术（上海）有限公司，为**外国法人独资**。
- 探探虽然关闭了Facebook功能，但在代码中依然**保留**了facebook SDK。

隐蔽传输



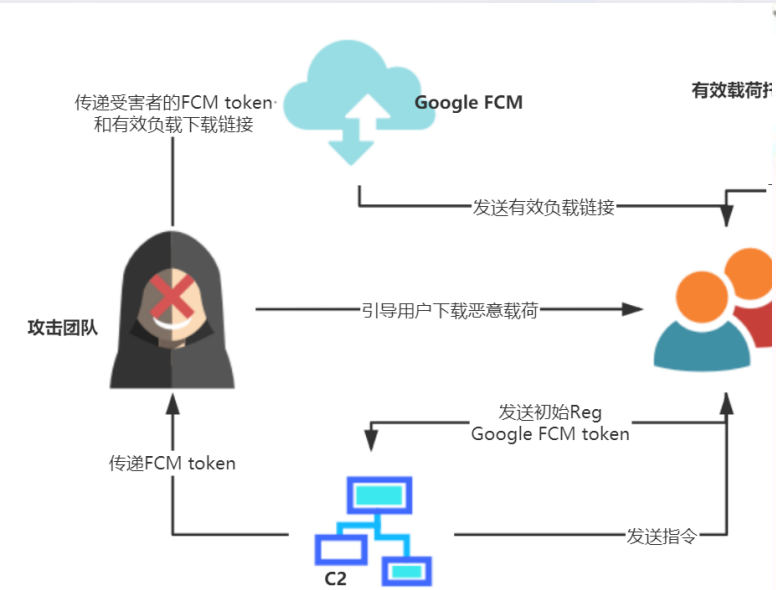
隐私声明模糊化、隐蔽共享传输可能

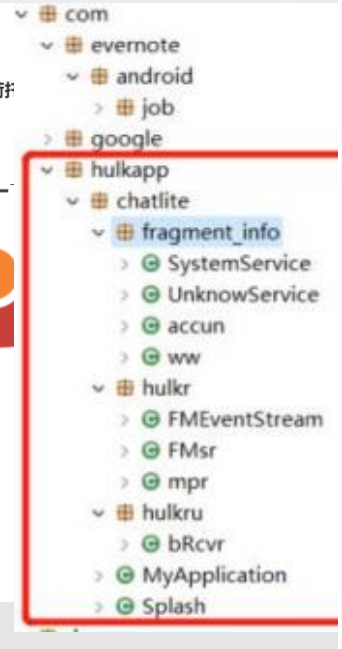
- 分析师发现小红书Amazon亚马逊国内运营商并未给出详细的条款来说明如何对**数据跨境**访问进行**保护**
- 在 inmobi 的隐私协议中提到：个人信息可能进行**出售或转让**
- 在国际数据传输的表述中，他们声明用户的**个人信息**可被**跨国进行访问**和**处理**
- 探探隐私声明中明确声明集成了较多第三方SDK，且多具有**数据收集和回传能力**

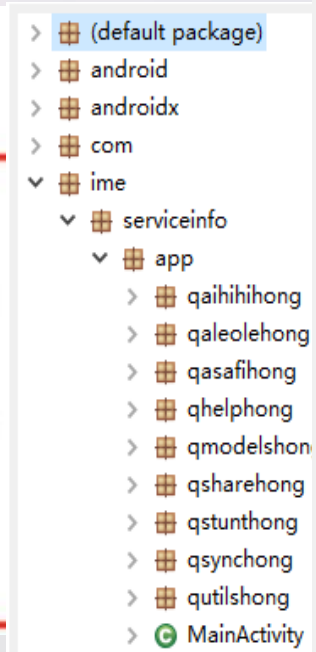
03 移动端高级威胁发现

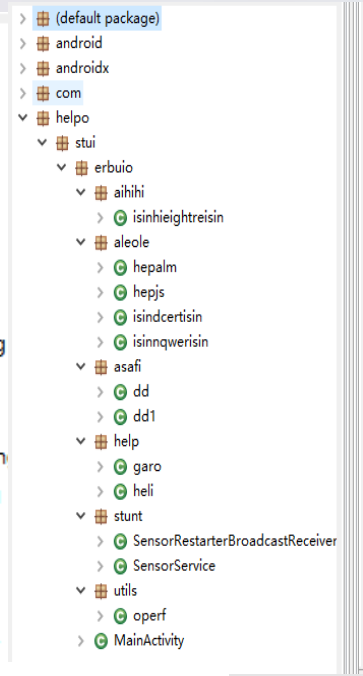
持续发现DoNot组织发起的攻击事件

样本图标	
文件类型	APK
样本名	System Service2
样本包名	com.tencent.mm
Hash	8A75B**********
开发者签名	emailAddress=andro d,O=Android,L=Mountair
入库时间	2020-05-13
病毒检出名	Trojan/Android.Donc
C2 服务器	rythemsjoy.club （存活）









利用自动化加密进行检测逃逸

```
try {
    v1_2.a(v2_1, v3_2, v4_3, v5_4, v6_3);
    this.a(ajt.a("HuiofcvdTkU="), ajt.a("bmV0aW5mby50eHQHuiofcvd="), v27, v19, isinnqwerisin.B.g);
    this.a(ajt.a("HuiofcvdQ1Q="), ajt.a("Y29udGFjdHMudHh0Huiofcvd"), v27, v19, isinnqwerisin.B.b);
    this.a(ajt.a("Q2FsbAHuiofcvd=="), ajt.a("HuiofcvdQ2FsbExvZ3MudHh0"), v27, v19, isinnqwerisin.B.a);
    this.a(ajt.a("U01THuiofcvd"), ajt.a("Huiofcvdc21zLnR4dA=="), v27, v19, isinnqwerisin.B.c);
    this.a(ajt.a("HuiofcvdVHJ1ZQ=="), ajt.a("HuiofcvdVHJ1ZS50eHQ="), v27, v19, isinnqwerisin.B.e);
    this.a(ajt.a("R1AHuiofcvd="), ajt.a("HuiofcvdR1AudHh0"), v27, v19, isinnqwerisin.B.k);
    this.a(ajt.a("HuiofcvdS2V5"), ajt.a("a2V5cy50eHHuiofcvdQ="), v27, v19, isinnqwerisin.B.d);
    this.a(ajt.a("TG12ZQHuiofcvd=="), ajt.a("TG12ZS50eHQ="), v27, v19, isinnqwerisin.B.h);
    this.a(ajt.a("HuiofcvdUEs="), ajt.a("cGtpbmZvLnR4dA=="), v27, v19, isinnqwerisin.B.l);
    this.a(ajt.a("Q0UHuiofcvd="), ajt.a("HuiofcvdY2UudHh0"), v27, v19, isinnqwerisin.B.m);
    this.a(ajt.a("QlcHuiofcvd="), ajt.a("YncudHh0"), v27, v19, isinnqwerisin.B.n);
    if(isinnqwerisin.i) {
```

利刃鹰组织仿冒微信在一带一路地区发起移动端攻击

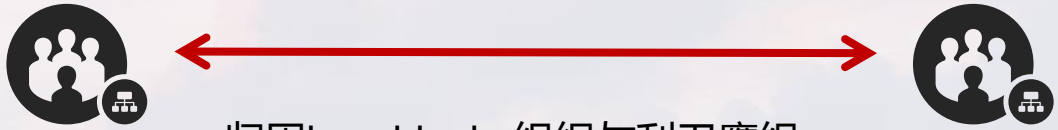
WeChat

4E804FB1F27598E1CAB555769D9A71EC

包名	com.example.dat.a8andoserverx
病毒名	Trojan/Android.bhdfhh.a[prv,rmt,spy,gen]
程序版本	1
上架市场	-
组织标签	利刃鹰BladeHawk

sample_hash:4E804FB1F27598E1CAB555769D9A71EC

2021-02-06 18:54:14 黑样本 DL0



归因kasablanka组织与利刃鹰组织
为同一组织

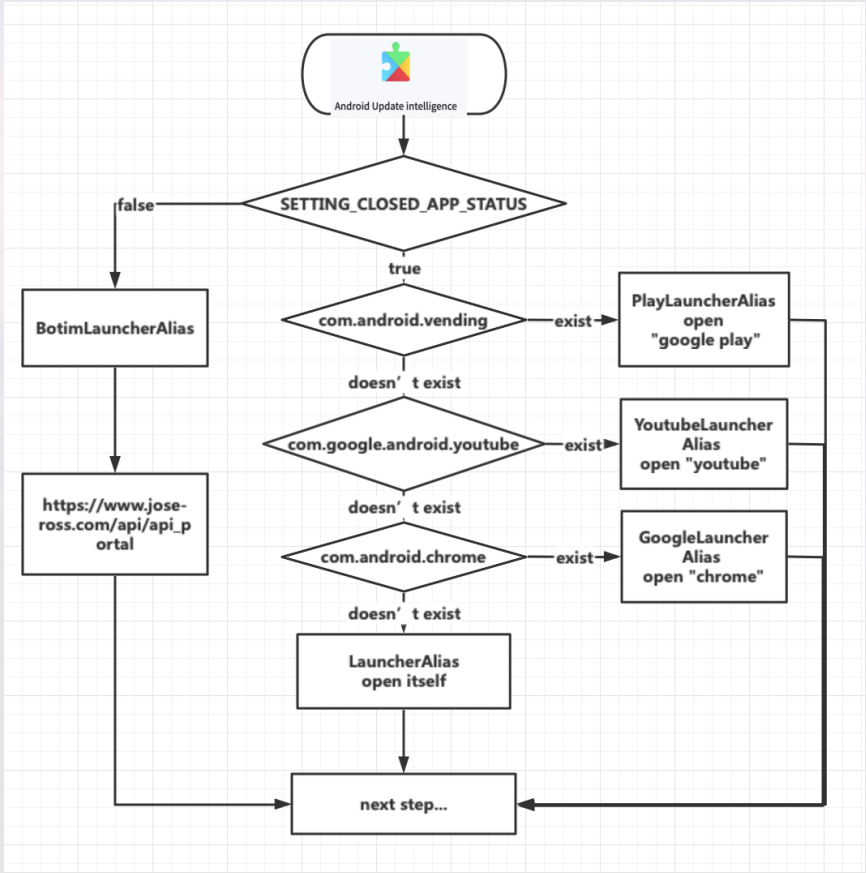
样本还集成了专门钓鱼Facebook账号的功能。钓鱼模块则被写在Activity2中，用于窃取受害者的Facebook登录凭证。

```
if(Activity2.this.fffesq.length() > 0 && Activity2.this.fffesq2.length() > 0) {
    try {
        StringBuilder v1 = new StringBuilder();
        v1.append(Environment.getExternalStorageDirectory().getPath());
        v1.append("/DCIM/.fdat");
        Activity2.this.out = new BufferedWriter(new FileWriter(v1.toString(), true));
        BufferedWriter v1_1 = Activity2.this.out;
        v1_1.write("User : " + Activity2.this.fffesq + "@8&@Pass : " + Activity2.this.fffesq2 + "@8&@@8&@");
        Activity2.this.out.close();
    }
    catch(IOException v0) {
    }
    catch(FileNotFoundException v0_1) {
    }

    try {
        Intent v0_3 = Activity2.this.getPackageManager().getLaunchIntentForPackage("com.facebook.katana");
```

发现双尾蝎组织攻击事件


```
Log.e(v9_1, v0_1.toString());
if(f.G(this.t).equalsIgnoreCase(d.a.a.e.a.k)) {
    v9_1 = "com.android.vending";
}
else if(f.G(this.t).equalsIgnoreCase(d.a.a.e.a.l)) {
    v9_1 = "com.google.android.youtube";
}
else if(f.G(this.t).equalsIgnoreCase(d.a.a.e.a.m)) {
    v9_1 = "com.android.chrome";
}
else {
    v9_1 = "app.lite.bot";
}
```



APT37攻陷国内防护较弱网站作为肉鸡服务器


```
v4, "/tencent/MicroMsg/WeiXin"
v5, "/Camera"
v6, "/Recordings"
v7, "/KakaoTalk"
v8, "/사진"
v9, "/Android/data/com.tencent.mm"
```

2021年移动高级威胁发现

1月份

apt37样本发现与分析

kbuster银行木马最新追踪

月光鼠组织移动活动分析

2月份

confucius样本发现与分析

3月份

利刃鹰样本发现与分析

卡萨布兰卡组织归因

4月份

持续补货肚脑虫样本分析

joker恶意样本分析

5月份

kimsuky样本分析

仿冒韩国安全软件样本分析

6月份

PJobRAT分析

goontact攻击活动追踪溯源

7月份

艾叶豹组织针对巴基斯坦的

意样本分析

pegasus木马专项分析

8月份

黄金鼠最新样本分析

利刃鹰最新样本分析

透明部落移动端攻击活动

追踪溯源

谢谢大家

安天冬训营 wtc.antiy.cn